Kristin L. Cleveland, OSB# 001318
Email: kristin.cleveland@klarquist.com
Salumeh R. Loesch, OSB# 090074
Email: salumeh.loesch@klarquist.com
John D. Vandenberg, OSB# 893755
Email: john.vandenberg@klarquist.com
KLARQUIST SPARKMAN, LLP
121 S.W. Salmon St., Ste. 1600
Portland, Oregon 97204
Telephone: (503) 595-5300
Facsimile: (503) 595-5301

Attorneys for Plaintiff
TRIPWIRE, INC.

UNITED STATES DISTRICT COURT
DISTRICT OF OREGON
PORTLAND DIVISION

TRIPWIRE, INC., Plaintiff, v. **UPGUARD, INC.,** Defendant.	Civil Case No.: 3:17-cv-0114 **COMPLAINT FOR PATENT INFRINGEMENT, TRADE SECRET MISAPPROPRIATION, AND INTERFERENCE WITH ECONOMIC RELATIONS** **DEMAND FOR JURY TRIAL**

For its Complaint against Defendant UpGuard, Inc. ("UpGuard" or "Defendant"), Plaintiff Tripwire, Inc. ("Tripwire"), through its attorneys, alleges as follows:

NATURE OF THE ACTION

1. This is a civil action for legal and equitable relief for infringement of United States Patent No. 7,316,016 ("the '016 patent"), misappropriation of trade secrets, and intentional interference with economic relations.

PARTIES

2. Plaintiff Tripwire is a corporation organized and existing under the laws of the state of Delaware, having its principal place of business at 101 SW Main St., Suite 1500, Portland, Oregon 97204.

3. On information and belief, UpGuard is a corporation organized and existing under the laws of the State of Delaware, having its principal place of business at 909 San Rafael Ave, Mountain View, California, 94043. On information and belief, UpGuard maintains an office in the state of Oregon at 10725 SW Barbur Blvd., Suite 120, Portland, OR 97219. On information and belief, UpGuard has appointed CT Corporation System, 388 State Street, Suite 420, Salem, Oregon 97301, as its agent for service of process in the state of Oregon.

JURISDICTION AND VENUE

4. This Court has jurisdiction over the subject matter of this action pursuant to 18 U.S.C. § 1836(c), and 28 U.S.C. §§ 1331, 1338(a) as to Tripwire's federal patent and trade secret claims. This Court has supplemental jurisdiction over Tripwire's state law claims pursuant to 28 U.S.C. § 1367(a) because those claims are so related to the claims in this action within the Court's original jurisdiction that they form part of the same case or controversy.

5. This Court has personal jurisdiction over UpGuard at least because UpGuard regularly conducts business in this judicial district, maintains a place of business in this judicial district, has employees in this judicial district, and has engaged in systematic and continuous contacts with the state of Oregon. Moreover, on information and belief, UpGuard has committed acts of patent infringement at issue in this action in this judicial district.

6. Venue is proper in this district pursuant to 28 U.S.C. §§ 1391 and 1400(b), because UpGuard transacts business in this district, has committed acts of patent infringement,

has misappropriated trade secrets and performed other tortious and wrongful acts in and impacting this district, and is subject to personal jurisdiction in this district.

FACTUAL BACKGROUND

7. Tripwire was founded in 1997. Today, Tripwire is recognized as a leading provider in the Security Vulnerability Management market.

8. On information and belief, UpGuard (formerly known as ScriptRock) was founded in 2012, and is a privately held, venture-funded company headquartered in Mountain View, California.

9. Tripwire and UpGuard compete for customers and employees.

10. Tripwire maintains certain confidential trade secrets, which include: (1) Tripwire's information about Tripwire's products, market analysis, and product requirements for enterprise security solutions, including without limitation integrity monitoring, configuration management, change audit, change control management, vulnerability detection, and vulnerability assessment, and identification of specific problems that Tripwire's products can and might in the future solve for the market and associated product requirements; (2) Tripwire's detailed data regarding Tripwire's current and prospective customers including customer lists, contact information, technology environments, feedback on existing and future solutions, and specific customer needs, Tripwire's information related to customer engagements, licensing arrangements, negotiated pricing and financial terms, Tripwire's information aggregated from customers related to industry-wide customer requirements and technology changes in the market; (3) Tripwire's information regarding Tripwire sales strategies and sales force assignments, employees, skills, performance, territories, compensation and sales compensation plan; (4) Tripwire's overall market analysis, including routes to market, pricing, product positioning,

competitive analysis, and segmentation and mapping of the needs for specific target markets; and (5) information and analysis related to Tripwire's product portfolio including: product features; product benchmarking; strengths and weaknesses; global pricing strategies including pricing models, schedules, guidelines and procedures; product specifications that deliver on market requirements; and product positioning for all target markets, buyers and customers.

11. Tripwire has dedicated significant resources to developing and protecting its trade secrets. For example, Tripwire has dedicated substantial time, money, and effort to develop and pinpoint those customers and potential contacts whose identities and unique organizational needs are not well-known or readily ascertainable in the market. Specifically, Tripwire has developed, *inter alia*, customer lists, specific customer contacts, contact information, pricing information, positioning information, and information about existing and prospective clients' needs, use-case scenarios, buying preferences and history, and network architectures (hereinafter, "Tripwire Confidential Customer Information"). This information, and its secrecy, provides Tripwire a significant business advantage by, *inter alia*, lowering its cost of customer acquisition relative to its competitors lacking this secret information.

12. Due to the value of this information's secrecy to Tripwire's success as a business, Tripwire makes substantial efforts to preserve and maintain the information in confidence. For example, Tripwire maintains such information in non-public, secured databases, such as its internal Salesforce database. By way of further example, only employees who have a need to access Tripwire's Salesforce database have such access, and each such individual has an individual log in and password to access the database.

13. Among other things, Tripwire requires employees with access to Tripwire's confidential and trade secret information to sign an agreement (the Employee Proprietary

Information And Inventions Agreement, hereinafter "Confidentiality Agreement") tailored to protect Tripwire's confidential and proprietary information ("Tripwire Proprietary Information"). A sample of a Confidentiality Agreement is attached hereto as Exhibit A. Employees are reminded of their obligations pursuant to the Confidentiality Agreement from time to time during their employment with Tripwire and upon leaving Tripwire. A sample of an obligation reminder is attached hereto as Exhibit B.

14. The Confidentiality Agreement: (1) requires that Tripwire Proprietary Information is held in the strictest confidence; and (2) prohibits use or disclosure of Tripwire Proprietary Information, both of which duties continue after employment ends. Ex. A (Confidentiality Agreement) at ¶ 1.1.

15. The Confidentiality Agreement prohibits employees who have left Tripwire from soliciting, for a one year period, other Tripwire employees to leave Tripwire. Ex. A (Confidentiality Agreement) at ¶ 4.

16. Tripwire Proprietary Information, per the Confidentiality Agreement, includes, without limitation, information regarding the skills and compensation of other employees of Tripwire, and information regarding plans for research, development, new products, marketing and selling, business plans, prices and costs, suppliers and customers. Ex. A (Confidentiality Agreement) at ¶ 1.2.

17. On information and belief, there are at least twelve (12) former Tripwire employees who, subsequent to working at Tripwire, now work or have worked at UpGuard.

18. At least the following employees, who were and are subject to the obligations set forth in the Confidentiality Agreement, have left Tripwire and joined UpGuard:

a. Norman Zulauf (joined Tripwire in February 2013, and left September 30, 2016; most recent title held at Tripwire: Enterprise Sales Manager; on information and belief, Mr. Zulauf is currently in a role at UpGuard similar to his role at Tripwire);

b. Tom Lynn (joined Tripwire in January 2010, and left September 16, 2016; most recent title held at Tripwire: VP Sales, Eastern Region; on information and belief, Mr. Lynn is currently in a role at UpGuard similar to his role at Tripwire);

c. Andy Steigleder (joined Tripwire in December 2005, and left August 12, 2016; most recent title held at Tripwire: Engagement Manager; on information and belief, Mr. Steigleder is currently an UpGuard Solutions Architect, a role similar to his role at Tripwire);

d. Michael Lohr (joined Tripwire in June 2013, and left August 14, 2015; most recent title held at Tripwire: Enterprise Sales Manager; on information and belief, Mr. Lohr is currently an UpGuard Regional Sales Director, a role similar to his role at Tripwire); and

e. Tony Esposito (joined Tripwire in December 2005, and left November 28, 2014; most recent title held at Tripwire: VP Sales, North America; on information and belief, Mr. Esposito is currently UpGuard's Senior VP of Sales, a role similar to his role at Tripwire)

(hereinafter, "Tripwire Former Employees"). Each of these individuals had access to Tripwire Proprietary Information, including access to Tripwire's Salesforce database. Each of these individuals had access to Tripwire Confidential Customer Information. Each of these individuals

was provided a reminder of his obligations, pursuant to the Confidentiality Agreement, at the time he left Tripwire.

19. UpGuard is aware of the confidentiality obligations of at least some of the Tripwire Former Employees. On October 10, 2016, UpGuard received a letter from Tripwire detailing Mr. Lynn's obligations, pursuant to the Confidentiality Agreement associated with Mr. Lynn's obligations, and noting UpGuard's hiring Mr. Zulauf subsequent to hiring Mr. Lynn.

20. On information and belief, UpGuard has approximately 50 to 60 employees, and approximately 12 of those are former Tripwire employees.

21. On information and belief, UpGuard has begun a campaign to target Tripwire customers with, on information and belief, the assistance of former employees of Tripwire.

22. For example, UpGuard has approached several customers of Tripwire. On information and belief, UpGuard has used information supplied by former Tripwire employees, including Tripwire Confidential Customer Information, to directly compete with Tripwire.

23. UpGuard has aggressively targeted Tripwire's product in comparative advertising on UpGuard's website. UpGuard's website includes approximately 20 different product comparisons regarding Tripwire, whereas most other competitors are mentioned in only a few.

24. Tripwire invests heavily in innovation. In addition to protecting its investment by requiring confidentiality agreements and protecting its trade secrets, Tripwire holds 40 patents.

25. On January 1, 2008, the '016 patent, titled "Homogeneous Monitoring of Heterogeneous Nodes," was duly and legally issued by the United States Patent and Trademark Office. A true and correct copy of the '016 patent is attached hereto as Exhibit C.

26. Tripwire is the owner by assignment of the '016 patent and, without limitation, has the rights to sue and collect damages for all past, present or future infringement.

COUNT I

(Infringement of U.S. Patent No. 7,316,016)

27. Tripwire re-alleges the foregoing paragraphs 1-26 as if fully set forth here.

28. On information and belief, UpGuard has infringed and is still infringing the ’016 patent by at least using and selling, in the United States, without a license or authority, the UpGuard platform, which monitors a system or network comprising a plurality of heterogeneous nodes. The UpGuard platform infringes at least claims 1, 3, 4, 5, 6, and 13 of the ’016 patent.

29. As a non-limiting example, UpGuard’s use of the UpGuard platform on computers under the control of UpGuard infringes claim 1 of the ’016 patent. Claim 1 is a “computerized method of monitoring a system or network comprising a plurality of heterogeneous nodes.” The UpGuard platform provides “complete visibility into the configuration of every server, network device, and cloud app you’re running,” and is “capable of scanning servers, websites, cloud hosts and network devices.” *See* https://www.upguard.com/features, and https://www.upguard.com/blog/upguard-an-adaptable-nerc-compliance-solution. The nodes that the UpGuard platform monitors include a wide variety of different nodes, including “anything with an IP address.” *See* https://support.upguard.com/upguard/nodes.html. To the extent that the preamble is construed as a limitation, this limitation has been met.

a. Claim 1 recites “defining multiple rules, each of the rules identifying criteria for detecting when the plurality of heterogeneous nodes on the system or network deviate from an authoritative state.” The UpGuard platform provides “policies” that include rules that specify criteria for detecting when scanned nodes associated with the policy are not in their “desired configuration state.”

In addition, the policies supported by the UpGuard platform provide customizable "checks" and "attribute checks" that specify rules for detecting when a scanned node deviates from a desired state. *See* https://support.upguard.com/upguard/policies.html. UpGuard performs the recited functionality; this limitation has been met.

b. Claim 1 requires "defining multiple logical groupings of one or more heterogeneous nodes, the logical groupings determining where the rules are applied." The UpGuard platform defines "node groups." In the UpGuard platform, "[p]olicies are always applied to node groups." *See* https://support.upguard.com/upguard/policies.html. UpGuard performs the recited functionality; this limitation has been met.

c. Claim 1 recites "defining multiple monitoring tasks, each monitoring task comprising applying at least one of the rules to at least a subset of a logical grouping of heterogeneous nodes." As an example, by default, node groups monitored by the UpGuard platform are set to be scanned repeatedly; the platform details configuration changes and the policies are applied to produce pass/fail results. *See* https://support.upguard.com/upguard/reporting.html. UpGuard performs the recited functionality; this limitation has been met.

d. Claim 1 recites "executing the multiple monitoring tasks." The UpGuard platform executes multiple monitoring tasks by, *inter alia*, performing scan(s), and producing policy pass/fail results for one or more active policies. *See* https://support.upguard.com/upguard/reporting.html. The UpGuard platform tracks the status of jobs. Tasks associated with a given job have status values,

including "pending," "processing," "assigned," "offline," and "actioned." *See* https://support.upguard.com/upguard/jobs-api-v2.html. UpGuard performs the recited functionality; this limitation has been met.

e. Claim 1 recites "in response to detecting a heterogeneous node deviating from the authoritative state, applying a remediation response wherein the remediation response is capable of both updating the authoritative state of the heterogeneous node and restoring the authoritative state of the heterogeneous node." The UpGuard platform executes multiple monitoring tasks by, *inter alia*, performing scan(s), and producing policy pass/fail results for one or more active policies. In response to a failing policy, the UpGuard platform provides for either updating the policy to reflect the new state (thereby updating the authoritative state of the heterogeneous node) or returning the failing node to a state that satisfies the policy (thereby restoring the authoritative state of the heterogeneous node). The UpGuard platform provides for both responses. For instance, "[a]s you update your configuration state, however, you need your policies to change to current." Also, the UpGuard platform not only provides a "suggested field to leave instructions on what to do if the policy is failing" but also provides for the automatic generation of "automation snippets" to produce "exactly the code [one] needs to make sure that the [deviating element] is the same as the rest of the group." UpGuard performs the recited functionality; this limitation has been met.

f. Claim 1 recites "wherein the one or more monitoring tasks are scheduled for opportunistic execution at a future date by an available one of the

heterogeneous nodes." The UpGuard platform tracks the status of jobs, and assigns a value to each, such as "pending," "processing," "success," or "failure." *See* https://support.upguard.com/upguard/jobs-api-v2.html. Tasks associated with a given job can have status values including "pending," "processing," "assigned," "offline," and "actioned." *See id.* The UpGuard platform's monitoring tasks are scheduled for opportunistic execution. UpGuard performs the recited functionality; this limitation has been met.

30. As a non-limiting example, the UpGuard platform infringes claim 3 of the '016 patent. Claim 3 is dependent on claim 1. Tripwire incorporates by reference the allegations of Paragraph 29. Claim 3 recites "the plurality of heterogeneous nodes comprise one of an active node-type or a passive node-type." Among the nodes that the UpGuard platform supports are servers, which are active. Among the nodes that the UpGuard platform supports are routers, which are passive. *See* https://www.upguard.com/discover. UpGuard performs the recited functionality; this limitation has been met.

31. As a non-limiting example, the UpGuard platform infringes claim 4 of the '016 patent. Claim 4 is dependent on claim 3. Tripwire incorporates by reference the allegations of Paragraph 30. Claim 4 recites "the one or more monitoring tasks are executed by an active node-type node." Among the nodes that the UpGuard platform supports are servers, which are active. *See* https://www.upguard.com/discover. UpGuard performs the recited functionality; this limitation has been met.

32. As a non-limiting example, the UpGuard platform infringes claim 5 of the '016 patent. Claim 5 is dependent on claim 3. Tripwire incorporates by reference the allegations of Paragraph 30. Claim 5 recites "the active node-types comprise at least one of a server, desktop

computer, laptop computer, set-top box, PDA and a cell phone." Among the nodes that the UpGuard platform supports are servers, which are active. *See* https://www.upguard.com/discover. UpGuard performs the recited functionality; this limitation has been met.

33. As a non-limiting example, the UpGuard platform infringes claim 6 of the '016 patent. Claim 6 is dependent on claim 3. Tripwire incorporates by reference the allegations of Paragraph 30. Claim 6 recites "the passive node types comprise at least one of a router, a switch, a sensor, a file, a directory, and a network port." Among the nodes that the UpGuard platform supports are routers, which are passive. *See* https://www.upguard.com/discover. UpGuard performs the recited functionality; this limitation has been met.

34. As a non-limiting example, the UpGuard platform infringes claim 13 of the '016 patent. Claim 13 is a "computerized method of monitoring a system or network comprising a plurality of heterogeneous nodes." The UpGuard platform provides "complete visibility into the configuration of every server, network device, and cloud app you're running," and is "capable of scanning servers, websites, cloud hosts and network devices." *See* https://www.upguard.com/features, and https://www.upguard.com/blog/upguard-an-adaptable-nerc-compliance-solution. The nodes that the UpGuard platform monitors include a wide variety of different nodes, including "anything with an IP address." *See* https://support.upguard.com/upguard/nodes.html. To the extent that the preamble is construed as a limitation, this limitation has been met.

a. Claim 13 recites "defining multiple rules, each of the rules identifying criteria for detecting when the plurality of heterogeneous nodes on the system or network deviate from an authoritative state." The UpGuard platform provides

"policies" that include rules that specify criteria for detecting when scanned nodes associated with the policy are not in their "desired configuration state." In addition, the policies supported by the UpGuard platform provide customizable "checks" and "attribute checks" that specify rules for detecting when a scanned node deviates from a desired state. *See* https://support.upguard.com/upguard/ policies.html. UpGuard performs the recited functionality; this limitation has been met.

b. Claim 13 recites "defining multiple logical groupings of one or more heterogeneous nodes, the logical groupings determining where the rules are applied." The UpGuard platform defines "node groups." In the UpGuard platform, "[p]olicies are always applied to node groups." *See* https://support.upguard.com/upguard/policies.html. UpGuard performs the recited functionality; this limitation has been met.

c. Claim 13 recites "defining multiple monitoring tasks, each monitoring task comprising applying at least one of the rules to at least a subset of a logical grouping of heterogeneous nodes." As an example, by default, node groups monitored by the UpGuard platform are set to be scanned every 24 hours (thus resulting in multiple monitoring tasks at each 24 hour period); the platform details configuration changes and the policies are applied to produce pass/fail results. *See* https://support.upguard.com/upguard/reporting.html. UpGuard performs the recited functionality; this limitation has been met.

d. Claim 13 recites "executing the multiple monitoring tasks." The UpGuard platform executes multiple monitoring tasks by, *inter alia*, performing scan(s),

and producing policy pass/fail results for one or more active policies. *See* https://support.upguard.com/upguard/reporting.html. The UpGuard platform tracks the status of jobs, and assigns a value to each, such as "pending," "processing," "success," or "failure." *See* https://support.upguard.com/upguard/jobs-api-v2.html. Tasks associated with a given job can have status values including "pending," "processing," "assigned," "offline," and "actioned." *See id.* UpGuard performs the recited functionality; this limitation has been met.

e. Claim 13 recites "in response to detecting a heterogeneous node deviating from the authoritative state, applying a remediation response wherein the remediation response is capable of both updating the authoritative state of the heterogeneous node and restoring the authoritative state of the heterogeneous node." The UpGuard platform executes multiple monitoring tasks by, *inter alia*, performing scan(s), and producing policy pass/fail results for one or more active policies. In response to a failing policy, the UpGuard platform provides for either updating the policy to reflect the new state (thereby updating the authoritative state of the heterogeneous node) or returning the failing node to a state that satisfies the policy (thereby restoring the authoritative state of the heterogeneous node). The UpGuard platform provides for both responses. For instance, "[a]s you update your configuration state, however, you need your policies to change to current." Also, the UpGuard platform not only provides a "suggested field to leave instructions on what to do if the policy is failing" but also provides for the automatic

generation of "automation snippets" to produce "exactly the code [one] needs to make sure that the [deviating element] is the same as the rest of the group." UpGuard performs the recited functionality; this limitation has been met.

f. Claim 13 recites "wherein the one or more monitoring tasks are scheduled for execution by an identified one of the heterogeneous nodes." The UpGuard platform tracks the status of jobs, and assigns a value to each, such as "pending," "processing," "success," or "failure." *See* https://support.upguard.com/upguard/jobs-api-v2.html. Tasks associated with a given job can have status values including "pending," "processing," "assigned," "offline," and "actioned." *See id.* The UpGuard platform's monitoring tasks are scheduled; for instance, the monitored environment is "scanned by default every 24 hours after which an email report is sent . . . detailing configuration changes and policy pass/fail results." *See, e.g.*, https://support.upguard.com/upguard/reporting.html. UpGuard performs the recited functionality; this limitation has been met.

35. Each of the asserted claims of the '016 patent is directed to particular and tangible methods. For example, claim 13 recites a particular and tangible method of monitoring a special type of network of computers with particular types of monitoring tasks, detecting deviations from desired computer state and in reaction taking particular, tangible steps to remedy the problem and restore or update and thereby improve the state of the computer network, resulting in a better working computer network.

36. As a result of UpGuard's infringement, Tripwire has suffered irreparable harm and has no adequate remedy at law. UpGuard's acts of infringement of the '016 patent have

injured and will continue to cause irreparable harm to Tripwire unless and until this Court enters an injunction prohibiting further infringement.

37. As a result of UpGuard's infringement, Tripwire has suffered monetary damages, and Tripwire will continue to suffer such harm in the future unless UpGuard's infringement is enjoined by this Court. To compensate Tripwire for such infringement, the Court should award, in no event less than, a reasonable royalty for the use made of Tripwire's inventions by UpGuard, together with interest and costs as fixed by the Court.

38. All conditions precedent to this Count have occurred or been performed.

COUNT II

(Trade Secret Misappropriation; Civil Action under 18 U.S.C. § 1836)

39. Tripwire re-alleges the foregoing paragraphs 1-38 as if fully set forth here.

40. Tripwire is the owner of certain valuable trade secrets including, *inter alia*, Tripwire Confidential Customer Information.

41. These trade secrets are related to Tripwire's products and services that are used in interstate and foreign commerce.

42. Messrs. Zulauf, Lynn, and Steigleder, directly and indirectly, including through former Tripwire employees now employed by UpGuard, conducted dozens of customer meetings while employed by Tripwire for Tripwire's benefit. Those customer meetings were often subject to non-disclosure obligations, binding both Tripwire and the customer. The meetings were held for the purpose of Tripwire researching customer needs, understanding sales opportunities, identifying areas of potential future product development, and obtaining feedback on Tripwire's product portfolio and product pricing. The information gathered and analyzed pursuant to these

meetings is a protected trade secret of Tripwire, included in the Tripwire Confidential Customer Information.

43. Messrs. Zulauf, Lynn, and Steigleder, while employed by Tripwire, had a need to access, and were provided secure access to, Tripwire Confidential Customer Information. This information is a protected trade secret of Tripwire.

44. Mr. Steigleder left Tripwire on August 12, 2016. He was provided a reminder of the obligations of the Confidentiality Agreement upon his departure. On information and belief, he became an UpGuard employee in August 2016.

45. Mr. Lynn left Tripwire on September 16, 2016. He was provided a reminder of the obligations of the Confidentiality Agreement upon his departure. On information and belief, he became an UpGuard employee in September or October 2016.

46. Mr. Zulauf left Tripwire on September 30, 2016. He was provided a reminder of the obligations of the Confidentiality Agreement upon his departure. On information and belief, he became an UpGuard employee in October 2016.

47. Tripwire expended considerable time, effort, and expense to compile Tripwire's trade secret information related to Tripwire's sales and marketing strategy, product strategy, customer needs, and technology innovation, including Tripwire Confidential Customer Information creating significant value for Tripwire.

48. The trade secrets are not known to the public and are not readily ascertainable by proper means to persons who could derive value from their disclosure or use.

49. Each of the Tripwire trade secrets mentioned herein, including the Tripwire Confidential Customer Information, derives independent economic value, actual and/or potential, from not being generally known to, and not being readily ascertainable through proper means by,

another person (such as UpGuard) who can obtain economic value from the disclosure or use of the information.

50. Tripwire undertook reasonable methods to maintain the secrecy of its confidential trade secret information including by (1) keeping the trade secret information in locked facilities and in locked, password-protected, and secure computer and network systems; (2) requiring non-disclosure agreements from non-employees exposed to the trade secret information; (3) ensuring limited access to trade secret information; and (4) requiring employees to maintain the confidentiality of all such information.

51. Tripwire entered into agreements with its employees, including Messrs. Zulauf, Lynn, and Steigleder, which specifically prohibited them from using or disclosing any Tripwire Proprietary Information, expressly including Tripwire's trade secrets, obtained in the course of their employment with Tripwire.

52. These trade secrets are of substantial economic value and have conferred a competitive advantage on Tripwire.

53. On information and belief, UpGuard has targeted current and former Tripwire employees in its hiring practices, and, currently, approximately one-quarter to one-fifth of UpGuard's workforce are former Tripwire employees.

54. On information and belief, UpGuard was aware, before and since hiring the former Tripwire employees, of the ongoing confidentiality obligations of the former Tripwire employees that now are employed by UpGuard. On information and belief, UpGuard knowingly induced those former employees to disclose to UpGuard and to use on behalf of UpGuard, Tripwire trade secrets and Proprietary Information, including Tripwire Confidential Customer Information.

55. On information and belief, Messrs. Zulauf, Lynn, and Steigleder knowingly misappropriated Tripwire's trade secrets, including Tripwire Confidential Customer Information, and disclosed it to UpGuard, which used such information to develop its technology, research, plans, products, marketing and selling strategies and materials, business plans, prices, costs, suppliers, customers, and/or operational practices, giving UpGuard the ability and opportunity to develop products to compete with Tripwire that it would not have been able to develop and launch on the same timeline without Tripwire's trade secret information.

56. UpGuard's knowledge of the trade secrets was derived from or through Tripwire Former Employees, who had acquired the trade secrets under circumstances giving rise to a duty to maintain the secrecy of the trade secrets; and owed and owe a duty to Tripwire to maintain the secrecy of the trade secrets.

57. Some of UpGuard's acts of trade secret misappropriation, including, without limitation, acquisition and use of Tripwire Confidential Customer Information, occurred on or after the date of the enactment of the Defend Trade Secrets Act, May 11, 2016.

58. For example, on information and belief, shortly after Mr. Lynn left Tripwire in September 2016, he approached, on behalf of UpGuard, a Tripwire customer to whom he had been introduced while a Tripwire employee and in his role as a Tripwire employee. Mr. Lynn, from his employment at Tripwire, was aware of Tripwire Confidential Customer Information regarding that customer, including the size and scope of the opportunity with that customer, the pricing information offered by Tripwire to that customer, the name and contact information for the individual customer contact, as well as the customer's specific technological needs.

59. On information and belief, Mr. Lynn, and other Former Tripwire Employees approached this and other Tripwire customers on behalf of UpGuard, offering the UpGuard platform, which infringes at least one Tripwire patent.

60. UpGuard's current and continued misappropriation of Tripwire's trade secrets is reckless and malicious. UpGuard knows of the confidentiality obligations and restrictions on use and disclosure of the trade secrets, by which the Tripwire Former Employees agreed to abide in the Confidentiality Agreement.

61. As a direct and proximate result of UpGuard's current and continued misappropriation of Tripwire's trade secrets, Tripwire will suffer imminent and irreparable harm.

62. Unless enjoined by this Court, UpGuard's acts of misappropriation will continue and Tripwire will continue to suffer irreparable harm.

63. Tripwire has no adequate remedy at law, and is entitled to an injunction under 18 U.S.C. § 1836(b)(3)(A).

64. On information and belief, UpGuard's continued use of these trade secrets is willful and malicious, and Tripwire is entitled to recover enhanced damages and its reasonable attorneys' fees under 18 U.S.C. §§ 1836(b)(3).

65. All conditions precedent to this Count have occurred or been performed.

COUNT III

(Violation of Oregon's Trade Secrets Act, ORS 646.461 et. seq.)

66. Tripwire incorporates by reference the allegations set forth in paragraphs 1 through 65.

67. Tripwire is the owner of certain valuable trade secrets including, *inter alia*, Tripwire Confidential Customer Information, stored in a secure and access-controlled database.

68. Messrs. Esposito, Zulauf, Steigleder, and Lynn, directly and indirectly, including through former Tripwire employees now employed by UpGuard, conducted dozens of customer meetings while employed by Tripwire for Tripwire's benefit. Those customer meetings were often subject to non-disclosure obligations, binding both Tripwire and the customer. The meetings were held for the purpose of Tripwire researching customer needs, understanding sales opportunities, identifying areas of potential future product development, and obtaining feedback on Tripwire's product portfolio. The information gathered and analyzed pursuant to these meetings is a protected trade secret, included Tripwire Confidential Customer Information.

69. Messrs. Esposito, Zulauf, Steigleder, and Lynn, while employed by Tripwire, had a need to access, and were provided secure access, to Tripwire Confidential Customer Information stored in its proprietary customer Salesforce database. This information is a protected trade secret.

70. The trade secrets are not known to the public and are not readily ascertainable by proper means to persons who could derive value from their disclosure or use.

71. Tripwire expended considerable time, effort, and expense to compile Tripwire's trade secret information related to Tripwire's sales and marketing strategy, product strategy, customer needs, and technology innovation, as well as ensuring Tripwire's products, pricing, and packaging creating significant value for Tripwire customers and partners.

72. Tripwire undertook reasonable methods to maintain the secrecy of its confidential trade secret information including by: (1) keeping the trade secret information in locked facilities and in locked, password-protected and secure computer and network systems; (2) requiring non-disclosure agreements from non-employees exposed to the trade secret

information; (3) ensuring limited access to trade secret information; and (4) requiring employees to maintain the confidentiality of all such information.

73. Messrs. Esposito, Zulauf, Steigleder, and Lynn acquired Tripwire's trade secret information pursuant to their positions with Tripwire, and in consideration of their signed Agreement to maintain confidentiality.

74. Tripwire entered into agreements with its employees, including Messrs. Esposito, Zulauf, Steigleder, and Lynn that specifically prohibited them from using or disclosing any Tripwire Proprietary Information, expressly including Tripwire's trade secrets, obtained in the course of their employment with Tripwire.

75. On information and belief, Messrs. Esposito, Zulauf, Steigleder, and Lynn, and other Former Tripwire Employees approached Tripwire customers on behalf of UpGuard, offering the UpGuard platform, which infringes at least one Tripwire patent.

76. On information and belief, Messrs. Esposito, Zulauf, Steigleder, and Lynn, and other Former Tripwire Employees used Tripwire Confidential Customer Information to UpGuard's advantage in offering the UpGuard platform.

77. These trade secrets and their secrecy are of substantial economic value and have conferred a competitive advantage on Tripwire.

78. On information and belief, Messrs. Esposito, Zulauf, Steigleder, and Lynn willfully misappropriated Tripwire's trade secrets and disclosed Tripwire's highly confidential trade secret information to UpGuard to help UpGuard develop its technology, research, plans, products, marketing and selling strategies and materials, business plans, prices, costs, suppliers, customers, and/or operational practices, giving UpGuard the ability and opportunity to develop

products to compete with Tripwire that it would not have been able to develop and launch on the same timeline without Tripwire's trade secret information.

79. On information and belief, UpGuard has targeted current and former Tripwire employees, including Messrs. Esposito, Zulauf, Steigleder, and Lynn, in its hiring practices and currently approximately one-fifth to one quarter of UpGuard's workforce are former Tripwire employees.

80. On information and belief, UpGuard was aware of the obligations of the former Tripwire employees that now are employed by UpGuard. On information and belief, UpGuard induced them to disclose Tripwire trade secrets and Proprietary Information.

81. Pursuant to ORS 646.465, Tripwire seeks damages, including both the actual loss caused by misappropriation, and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss, arising from UpGuard's misappropriation in an amount to be proven at trial and currently estimated at no less than $400,000, plus interest thereon at the statutory rate of 9%.

82. UpGuard's misappropriation as alleged herein was willful or malicious, and in disregard to Tripwire's statutory rights. Such conduct exceeds the bounds of social toleration and is of the type that punitive damages deter. Tripwire, therefore, reserves the right to amend this Complaint to seek punitive damages under ORS 646.465.

83. As a direct and proximate result of UpGuard's current and continued misappropriation of Tripwire's trade secrets, Tripwire will suffer imminent and irreparable harm.

84. Unless enjoined by this Court, UpGuard's acts of misappropriation will continue and Tripwire will continue to suffer irreparable harm.

85. Tripwire has no adequate remedy at law.

86. Tripwire has hired legal counsel to prosecute its claims and is entitled to recover from UpGuard its reasonable attorneys' fees under ORS 646.467.

87. All conditions precedent to this Count have occurred or been performed.

COUNT IV

(Intentional Interference with Economic Relations under Oregon Common Law)

88. Tripwire incorporates by reference the allegations set forth in paragraphs 1 through 87.

89. Until recently, Tripwire had employment contracts with several employees who are now UpGuard employees, including Messrs. Esposito, Zulauf, Steigleder, and Lynn. These agreements required that the employee not induce any other employee of Tripwire to leave Tripwire during the term of the employee's employment and for one year after leaving the company. The agreements also prohibited the employees from using or disclosing Tripwire Proprietary Information after their employment.

90. On information and belief, UpGuard has intentionally interfered with Tripwire's employment relationships with its employees by encouraging former Tripwire employees to recruit other Tripwire employees to leave Tripwire in favor of UpGuard.

91. On information and belief, UpGuard's intentional interference was undertaken for an improper purpose because it undertook the actions at issue to secure an unfair competitive advantage over Tripwire for UpGuard, to cause Tripwire to suffer economic losses, to cause Tripwire to incur expenses and lost productivity associated with replacing high-level and long-term employees, and to obtain additional Tripwire Proprietary Information by inducing some of Tripwire's employees to work for UpGuard.

92. Tripwire also had prospective contracts with several customer leads and contracts with at least one customer that is now an UpGuard customer.

93. On information and belief, UpGuard intentionally interfered with Tripwire's relationships with customers by inducing employees to use and disclose Confidential Information in pursuing business for UpGuard.

94. On information and belief, UpGuard's intentional interference was undertaken for an improper purpose because it undertook the actions at issue to secure an unfair competitive advantage over Tripwire for UpGuard, to cause Tripwire to suffer economic losses, to provide additional confidential and proprietary information to UpGuard and to use such information to secure customers for UpGuard.

95. On information and belief, UpGuard intentionally sought to damage Tripwire's ability to compete in the market with UpGuard and others through its actions.

96. UpGuard's intentional interference was undertaken by an improper means because: (1) on information and belief, former employees used confidential employee skill and compensation information in violation of the Confidentiality Agreement in order to induce employees to leave Tripwire's employ or to secure employment for employees at UpGuard; and (2) on information and belief, former employees engaged in a breach of contract when they induced the other employees to leave Tripwire to work for UpGuard.

97. As a direct and proximate result of UpGuard's actions as alleged herein, Tripwire has suffered economic damages reasonably to be expected from UpGuard's interference in an amount to be proved at trial and currently estimated at no less than $562,500, plus interest thereon at the statutory rate of 9%.

98. The actions of UpGuard as alleged herein were intentional, willful, and with reckless disregard to Tripwire's rights. Such conduct exceeds the bounds of social toleration and is of the type that punitive damages deter. Tripwire, therefore, reserves the right to amend this Complaint to seek punitive damages.

99. All conditions precedent to this Count have occurred or been performed.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Tripwire respectfully requests this Court to enter judgment against Defendant UpGuard granting the following relief:

A. The entry of judgment in favor of Tripwire and against Defendant;

B. A finding that Defendant has infringed claims of United States Patent No. 7,316,016;

C. An award of damages against Defendant adequate to compensate Tripwire for the infringement, but in no event less than a reasonable royalty as permitted under 35 U.S.C. § 284, together with prejudgment interest;

D. To the extent Defendant's infringement is found to be willful, a judgment that Tripwire is entitled to discretionary enhancement of its damages and other relief as provided by 35 U.S.C. § 284;

E. To the extent that this case is found to be exceptional, an award to Tripwire of its reasonable attorneys' fees, costs and expenses as permitted pursuant to 35 U.S.C. § 285;

F. A permanent injunction prohibiting further infringement by UpGuard, and each of its subsidiaries, successors, parents, affiliates, officers, directors, agents, servants, employees and all persons in active concert or participation with it;

G. A permanent injunction prohibiting Defendant from unfairly competing with Tripwire by using Tripwire's confidential and trade secret information misappropriated by the Former Tripwire Employees, including soliciting customers, using Tripwire Confidential Customer Information;

H. A permanent injunction prohibiting Defendant from unfairly competing with Tripwire by using Tripwire's confidential information misappropriated by the Former Tripwire Employees, to wrongfully interfere with Tripwire's contracts and economic relations with Tripwire employees;

I. A finding that Defendant has no right to use Tripwire's confidential information or trade secrets;

J. An award of compensatory damages in an amount not less than $562,500 for Defendant's unfairly competing with Tripwire by using Tripwire's confidential and trade secret information misappropriated by the Former Tripwire Employees, including soliciting customers, using Tripwire Confidential Customer Information;

K. An award of restitution;

L. Such other relief that Tripwire is entitled to under law and any other and further relief that this Court or a jury may deem just and proper.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Tripwire hereby demands a jury trial on all issues so triable in this action.

DATED: January 24, 2017

Respectfully submitted,

By: *s/ Kristin L. Cleveland*
Kristin L. Cleveland, OSB# 001318
Email: kristin.cleveland@klarquist.com

Salumeh R. Loesch, OSB# 090074
Email: salumeh.loesch@klarquist.com
John D. Vandenberg, OSB# 893755
Email: john.vandenberg@klarquist.com
KLARQUIST SPARKMAN, LLP
121 S.W. Salmon St., Ste. 1600
Portland, Oregon 97204
Telephone: (503) 595-5300
Facsimile: (503) 595-5301

Attorneys for Plaintiff
TRIPWIRE, INC.